REMARKS

The Examiner has maintained the current rejections. As set forth below, such new rejections are still deficient. However, despite such deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of multiple dependent claims into each of the independent claims. Since the subject matter of such dependent claims was already considered by the Examiner, it is asserted that such claim amendments would **not** require new search and/or consideration.

The Examiner has rejected Claims 1, 5-9, 13-17, and 21 under 35 U.S.C. 103(a) as being unpatentable over Hill et al. (U.S. Patent No. 6,088,804) in view of Chen et al. (U.S. Patent No. 5,960,170). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to include the subject matter of dependent Claims 2, 3 and 4 et al.

The Examiner has relied on the following excerpt from Hill to make a prior art showing of applicant's claimed "creating a histogram describing the specific event sequence occurrence for each of the applications" (see this or similar, but not identical, language in each of the foregoing claims):

> "**The mapping of display map** 66 (FIG. 4) is performed iteratively in a sequence of steps. Each step requires the presentation of one of training signatures 53, in the form of an input vector, **to the array of display cells 68** (each of display cells 68 being represented by a code vector). The input vector for one of training signatures 53 is used as an argument to an activation function that estimates the similarity between the input vector and each of the code vectors for display cells 68. The most similar code vector representing one of display cells 68 as well as its neighborhood of display cells 68 is adjusted to improve response to subsequent simulated attacks having similar training signatures.
>
> When another one of training signatures 53 is available, program control loops back to task 46 to access database 48, perform another one of simulated attacks 52, and map a vector representative of the training signature into display map 66.

When another one of training signatures 53 is not available, then training process 44 is exited with initial training complete." (Col. 7, lines 27-45-emphasis added)

Applicant respectfully asserts that the above excerpt from Hill fails to meet applicant's above mentioned claim language. Specifically, Hill simply discloses a "display map" with an "array of display cells" (see emphasized excerpt above). Furthermore, after considering the Figure referenced in the above excerpt, it is clear that Hill teaches a display map divided into regions and subregions that indicates attack type and attack severity (see Figure 4). This is clearly not a histogram, as claimed by applicant. Applicant argues that the plain and ordinary meaning of a histogram clearly departs from the display map of Hill.

In addition, after considering Figure 4 from Hill, it is clear that Hill also does not teach a histogram that "describ[es] the specific event sequence occurrence for each of the applications," as claimed by applicant. Figure 4, as referenced in the excerpt above, merely suggests a display map divided into regions and subregions that indicates attack type and attack severity, which does not rise to the level of specificity of applicant's "specific event sequence occurrence for each of the applications," as claimed.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite

such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has substantially incorporated the subject matter of Claims 2-4 et al. into each of the independent claims.

The Examiner has rejected Claims 2-4, 10-12 and 18-20 under 35 U.S.C. 103(a) as being unpatentable over Hill in view of Chen and in further view of Vaidya (U.S. Patent No. 6,279,113). Again, applicant respectfully disagrees with such rejection.

With respect to dependent Claim 2 et al., presently incorporated into each of the independent claims, the Examiner has relied on various excerpts from the Hill and Vaidya references to make a prior art showing of applicant's claimed "storage manager organizing the histograms into plurality of records ordered by object, application, and monitored event" (see this or similar, but not identical, language in each of the foregoing claims).

First, the Examiner has relied on Hill's disclosure of a "display map" (Col. 5, lines 26-65 and Col. 7, lines 27-54) to meet applicant's claimed "organizing histograms into a plurality of records." For substantially the same reasons as those given with respect to the independent claims, applicant respectfully asserts that Hill's "display map" does not meet applicant's claimed "histograms."

Second, the Examiner relies on Vaidya's disclosed "configuration generator 28 [that] is connected to the database handler to enable the network administrator to define the configuration of network objects on the LAN 11 and the remote network 24...Network objects further include applications and files stored in memory within those devices" (Col. 5, lines 45-66 and Col. 6, lines 1-56) to meet applicant's claimed "organizing the histograms into plurality of records ordered by...application..." Applicant respectfully asserts that simply defining the configuration of network objects where such objects include applications etc., as set forth in Vaidya, in no way meets organizing a histogram into a plurality of records ordered by application, as claimed.

With respect to dependent Claim 3 et al., presently incorporated into each of the independent claims, the Examiner has relied on the Hill and Vaidya references to make a prior art showing of applicant's claimed "structured database in which the plurality of records is stored; wherein the storage manager stores each histogram for each such specific event sequence occurrence in one such database record identified by the application by which the specific event sequence was performed" (see this or similar, but not identical, language in each of the foregoing claims).

Specifically, the Examiner has relied Hill's disclosed "display map" (Col. 5, lines 39-45 and Col. 7, lines 27-54) to meet applicant's claimed "wherein the storage manager stores each histogram for each such specific event sequence occurrence in one such database record..." For substantially the same reasons as those given with respect to the independent claims, applicant again respectfully asserts that Hill's "display map" does not meet applicant's claimed "histograms." Further, applicant also respectfully asserts that the Hill and Vaidya references also fail to teach the remaining limitations of applicant's claim language, namely "storing each histogram for each such specific event sequence occurrence in one such database record identified by the application by which the specific event sequence was performed" (emphasis added), for substantially the same reasons as those given with respect to the independent claims and dependent Claim 2 et al.

With respect to dependent Claim 4 et al., presently incorporated into each of the independent claims, the Examiner has relied on Figure 3 in Hill and Hill's disclosure of a task that compiles attack status information regarding a first attack (Col. 8, lines 30-50) and a task that predicts a pattern for subsequent attacks and adapts a security system to respond to subsequent attacks (Col. 9, lines 34-45) to meet applicant's claimed "wherein the storage manager configures the structured database as an event log organized by each event in the group of monitored events and updates the database record storing each specific event sequence occurrence with a revised histogram as each such occurrence is identified" (see this or similar, but not identical, language in each of the foregoing claims).

Again, applicant respectfully asserts that nowhere in Hill is there any teaching of a "histogram" as claimed by applicant, and especially not in the excerpts relied upon by the Examiner. In addition, merely adapting a security system according to predicted patterns of subsequent attacks in no way discloses "updating the database record storing each specific event sequence occurrence with a revised histogram as each such occurrence is identified," as claimed by applicant. Specifically, adapting a security system with predicted patterns of attacks simple does not meet "updating the database...with a revised histogram as each such occurrence is identified" (emphasis added).

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of applicant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Still yet, it is noted that the Examiner's rejections are also deficient with respect to the remaining dependent claims, since the references relied upon simply fail to teach or suggest all of the claim limitations. For example, with respect to dependent Claim 5 et al., the Examiner has relied on Hill's disclosed "SOM processor 40 [that] compares a vector representative of a first attack signature 94 (FIG. 6) to each of training signatures 53 as mapped in display map 66 (FIG. 4)" (Col. 8, lines 30-49) and "training signatures" (Col. 7, lines 46-54 and Col. 8, lines 30-49) to meet applicant's claimed "the analyzer detecting suspect activities within each histogram, each suspect activity comprising a set of known actions comprising a computer virus signature" (see this or similar, but not identical, language in each of the foregoing claims).

Applicant respectfully asserts that simply comparing attack signatures with training signatures that are mapped in a display map does not meet applicant's claimed "detecting suspect activities within each histogram" since Hill fails to teach both a

histogram and detecting suspect activities within a histogram. Specifically, Hill maps "only enough training signatures 53 to accurately portray a statistically significant number of attack types 76 (FIG. 4) into display map 66 (FIG. 4)" (Col. 7, lines 51-54). Hill simply does not teach detecting suspect activities within the display map.

Since at least the third element of the *prima facie* case of obviousness has not been met, a notice of allowance or a specific prior art showing of all of the claim limitations, in the context of the remaining elements, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P371/99.053.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100